Deployable DNS

Ray Buschur

21 August 2001

Organization: W114
Project: 0701A340-AT

MITRE

Agenda

- Background
- Task
- General Approach
- Domain Stability
- Address Space
- DNS Products
- Network Address Translation (NAT)
- Current Recommendation
- Where we are going

FY 00 Situation

- Existing SBU user community deployment senario
  - Address space provided ad-hoc by JTF/Theater/Unit
    - May include using sustaining base address space
  - JTF/Exercise assigned unique domain names
- Army stands up Window 2000 working group
- GCSS-A was scheduled to field a large Microsoft Windows 2000 infrastructure
  - Requires stable domain name
- Address space to support the deployed SBU user community
  - Plans to use SIPRNET address space were rejected
  - No standardized approach
- PEO C3S was not tasked to provide SBU solution until FY '04

Task

- Develop a proposal to resolve the current lack of DNS support the PEO STAMIS user community
  - Schedule permitting, develop a prototype of the recommended solution
- Three primary programs identified as essential GCSS-A, MC4, and SIDPERS-3 (AHRS)
  - Scope increased to include other systems

General Approach

- IP Address space was the most critical resource associated with the task, and was designated the primary driver for all recommendations
  - Each computer has to have an address to be on the network
- Six addressing schemes considered
  - Public IPv4 Class B network
  - Public IPv4 Class C network
  - Public IPv6 network
  - Private IPv6 network
  - Shared address space (garrison & Signal Center)
  - Private IPv4 network - Still working this approach
- Collect System Information
- Review candidate DNS solutions
- Finalize recommendations
- Present final recommendations

Domain Stability

- Windows 2000 and PKI (device certificates) require stable domain name
- Control of name and address space by deployable units
  - Discussing the control of DNS name and address space with ASC, generally receptive to unit control
  - Currently each deployable unit's name and address space is managed differently
  - Units must assume control of their DNS data
    - Assumption of control can be labor and time intensive process
  - MITRE is investigating the feasibility of including the deployable units in Army's DNS architecture similarly to the method used to include separate theaters now

Address Space

- Army Domain Manager issued Signal Center a class B network
  - Support the deployable SBU address space requirement
- Signal Center is currently allocating 16 class C sub-networks directly to each Corp and several MACOMs
  - Corps and MACOM distribute address space at their own discretion
  - Does not guarantee the deployable units specific amounts of address space
  - Signal Center is working with units to resolve issues
- Supported a Signal Center request to participate in a discussion on tactical address space and DNS services on 30-31 July

DNS Products Evaluated

- Scope of the implementation is restricted to the size of the deployable unit
  - Corp HQ & Corps support elements
  - Division
  - Separate brigades
- Nortel Networks - NetID
  - Rejected vender phasing out the product
- Lucent QIP - Commercial version
  - Viewed requirements to field product differently than PEO C3S
  - Rejected as not suitable for the task
    - Data replication was not supported within the product
    - User interface very difficult to use and understand
- Windows 2000 DNS using Active Directory
  - Installing and performing initial tests

Network Address Translation (NAT)

- Used to translate private un-routable IPv4 address space to routable IPv4 address space
- Application Level Gateways are used to proxy applications that transmit network specific information through connections

NAT Benefits

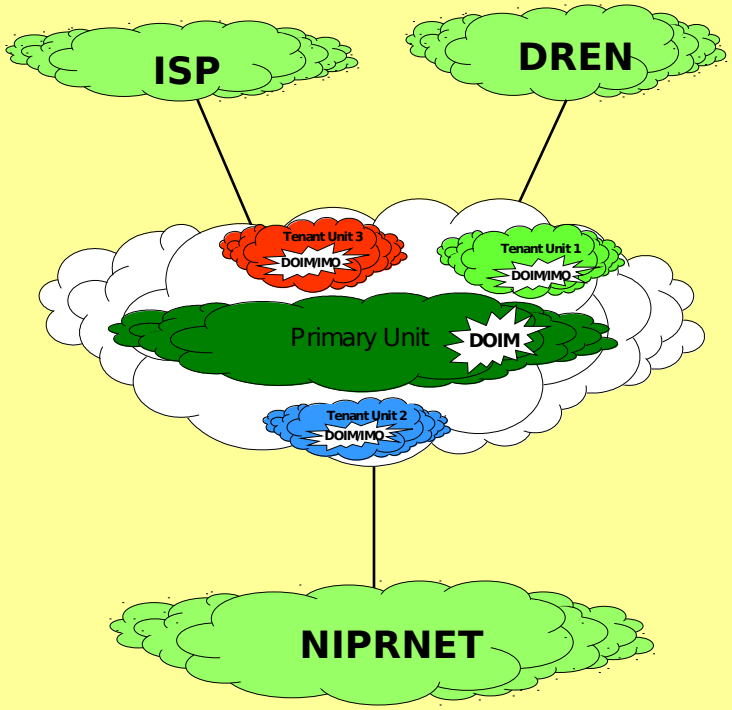
- Optimizes the utilization of public or routable IP address space
  - Sun claims one Class C network can support a well populated Class B network
- Enhances network security posture
  - Requires a closed enclave with well defined entry/exit points
  - Enclave is less susceptible to probing and follow-up attacks when few or no static mappings exist between the public and private enclaves

NAT Problems

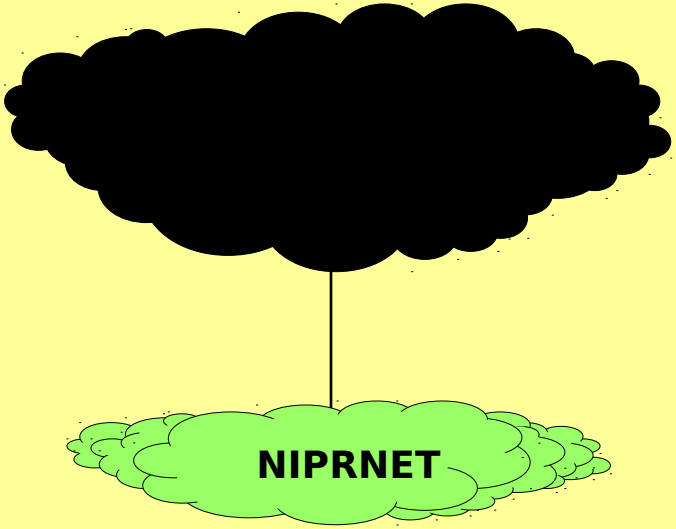
- Enclave hosts that must be known outside the enclave, must be statically mapped at the the NAT Server
  - Static mapping are manually created in most NAT servers
  - Efficiency of address space utilization decreases as the number of static mappings increase
- Two DNS systems must be maintained and synchronized
  - Public DNS is publicly accessible, contains references to only public or routable address space
  - Private DNS is only accessible from within the private enclave, may contain references to both public and private address space
- Enclave manager loses the ability to easily discriminate on an individual host basis, outside the enclave
  - NAT server allocation logs must be reviewed to determine which internal host was mapped to which external address at any given point

Enclave Types

- Public

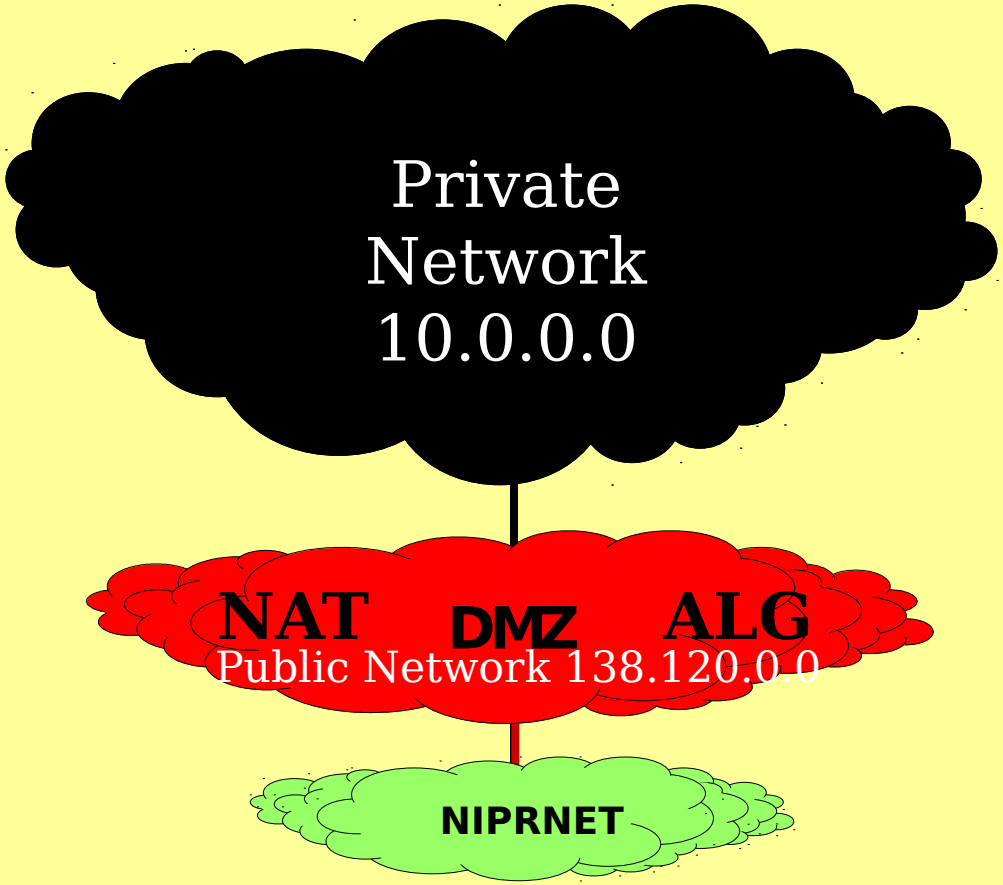


- Private

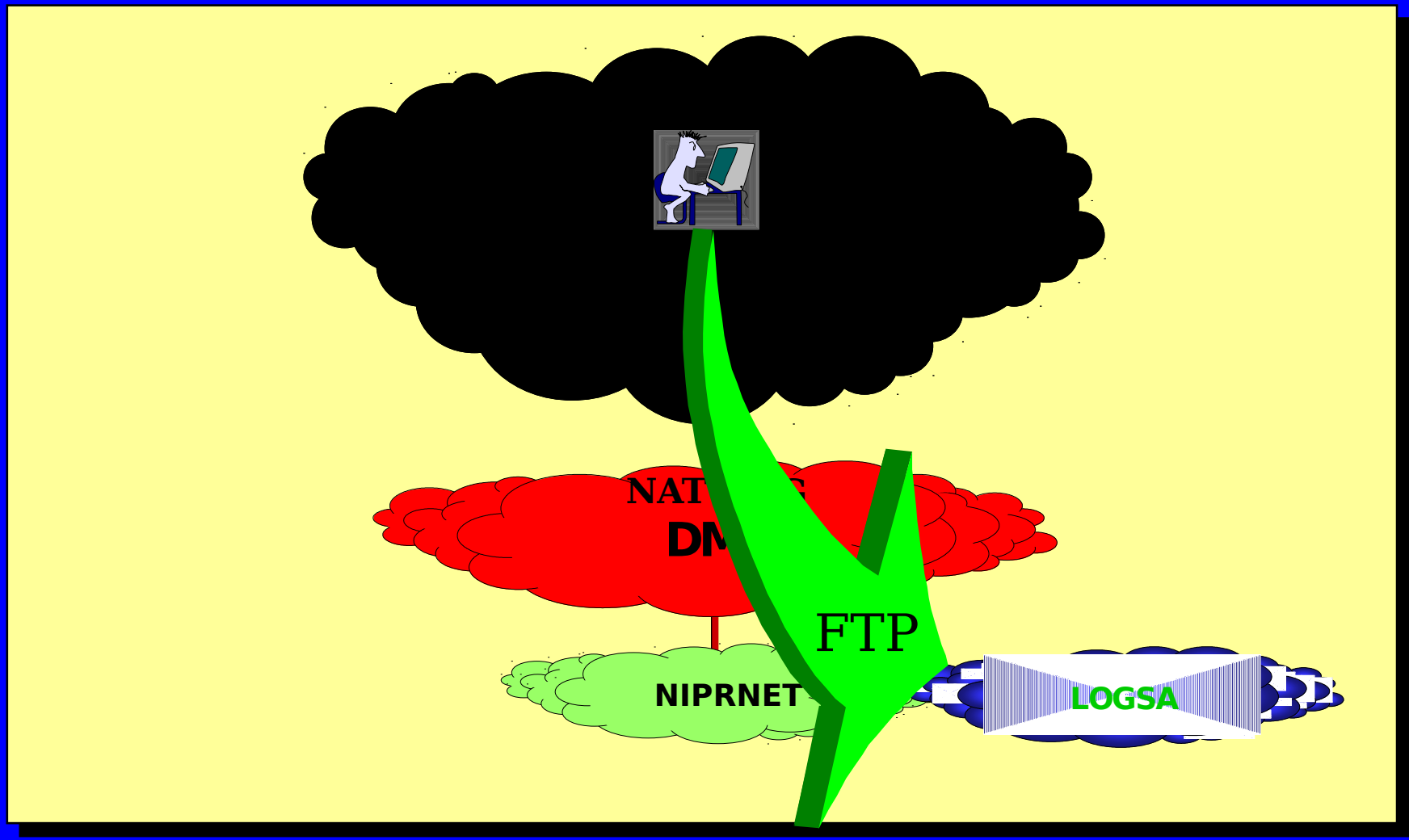


MITRE

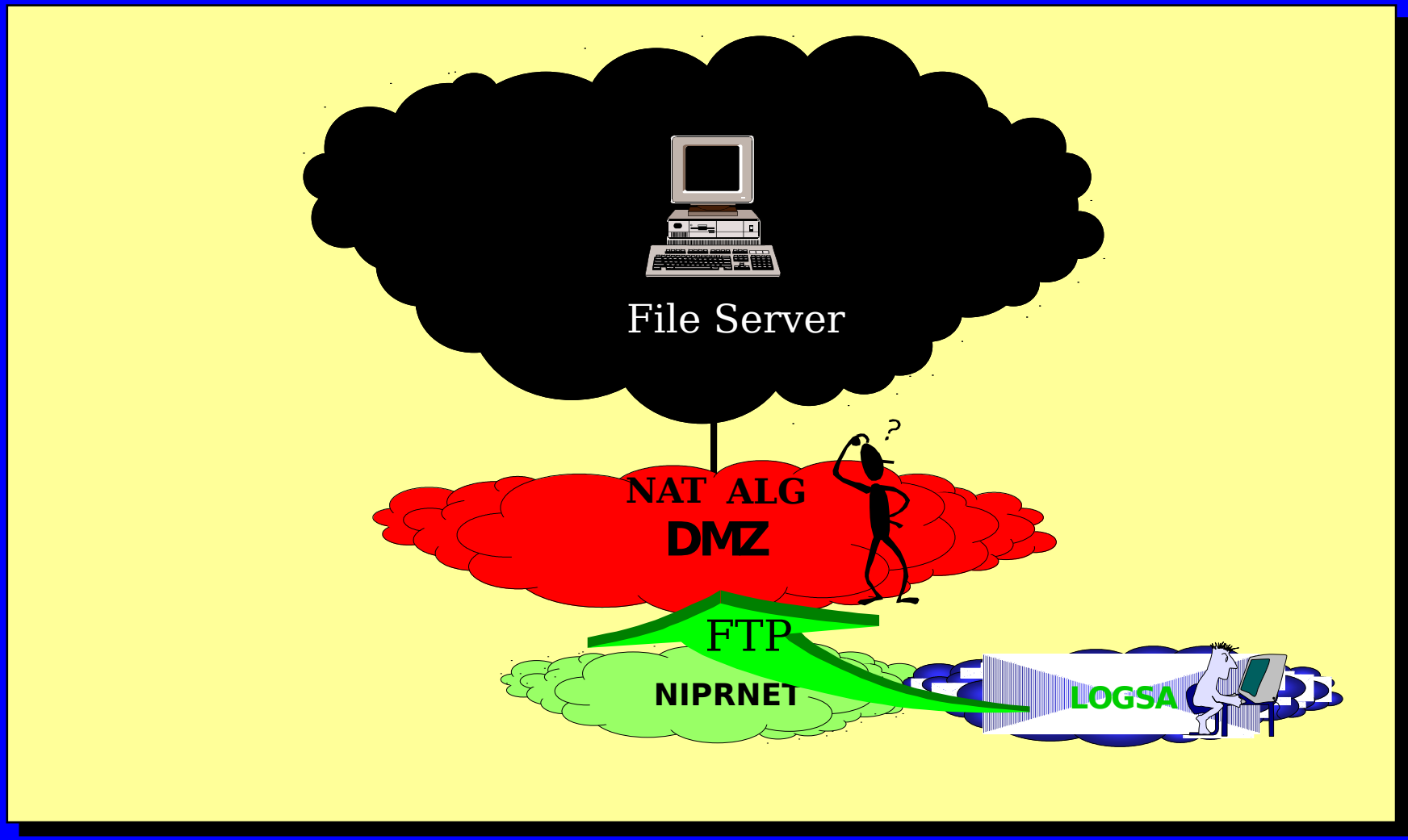
Private Enclave



Users Inside Private Enclaves

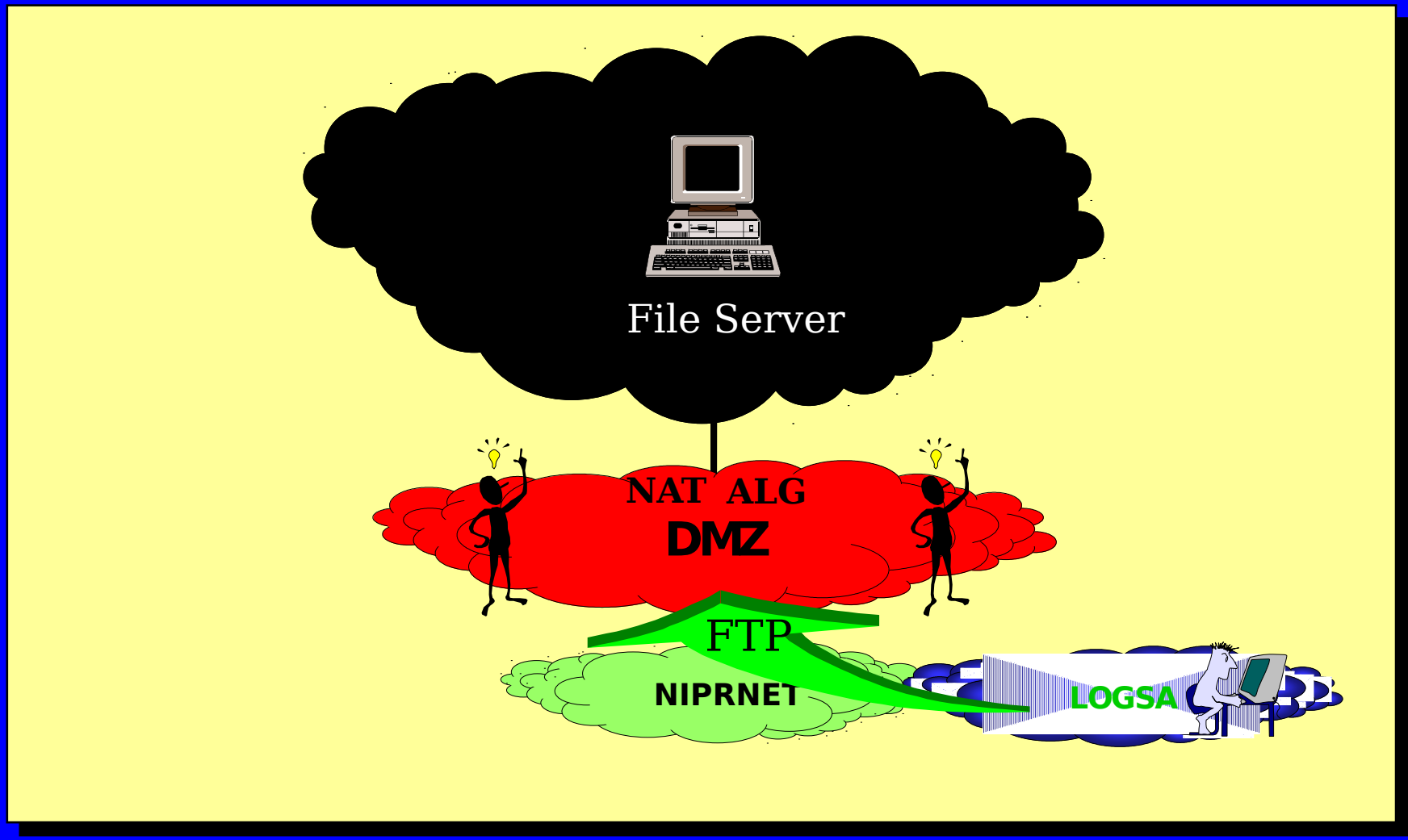


External Users Accessing Private Enclaves

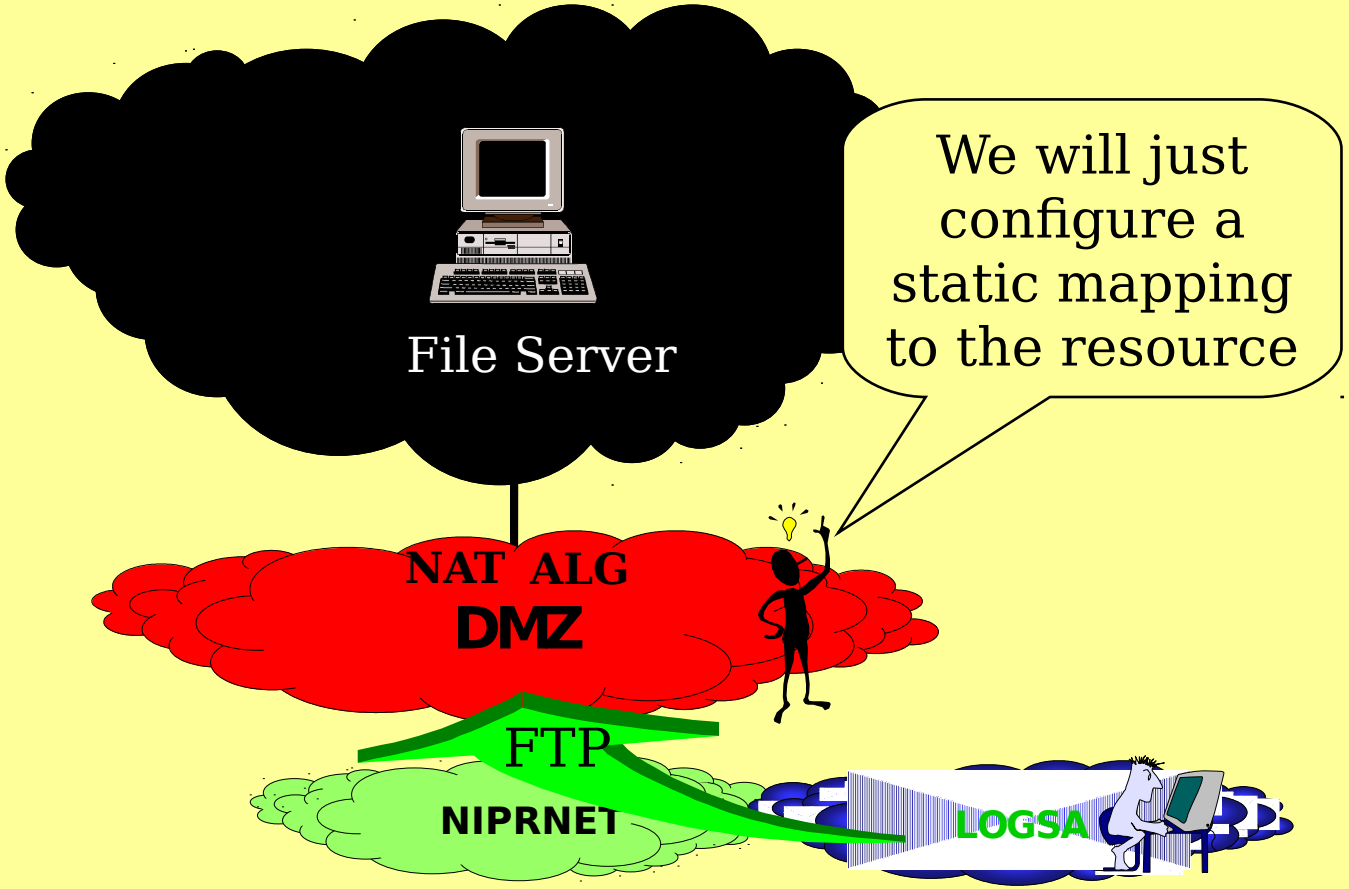


MITRE

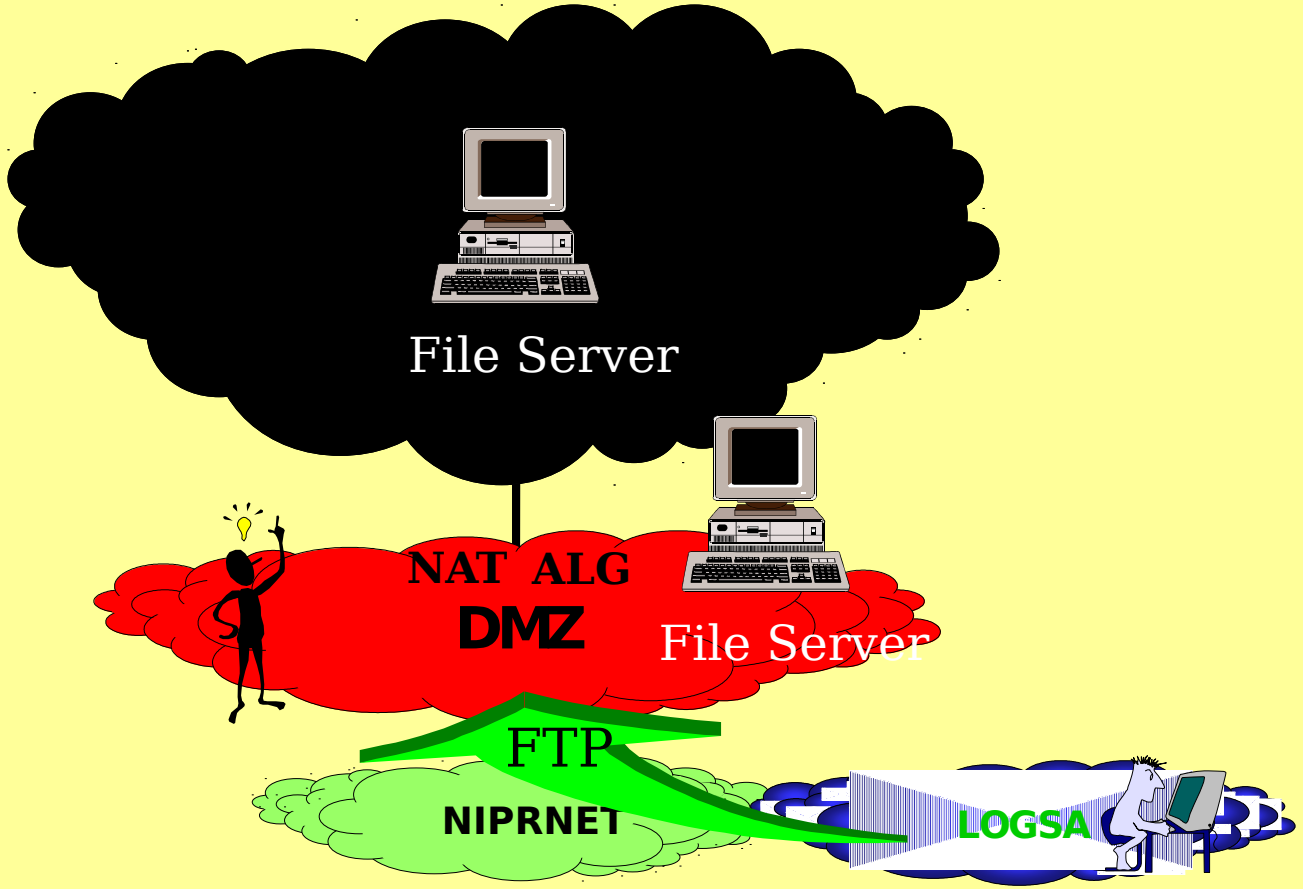
External Users Accessing Private Enclaves



External Users Accessing Private Enclaves
Resources Inside the Enclave



External Users Accessing Private Enclaves
Resources in the DMZ



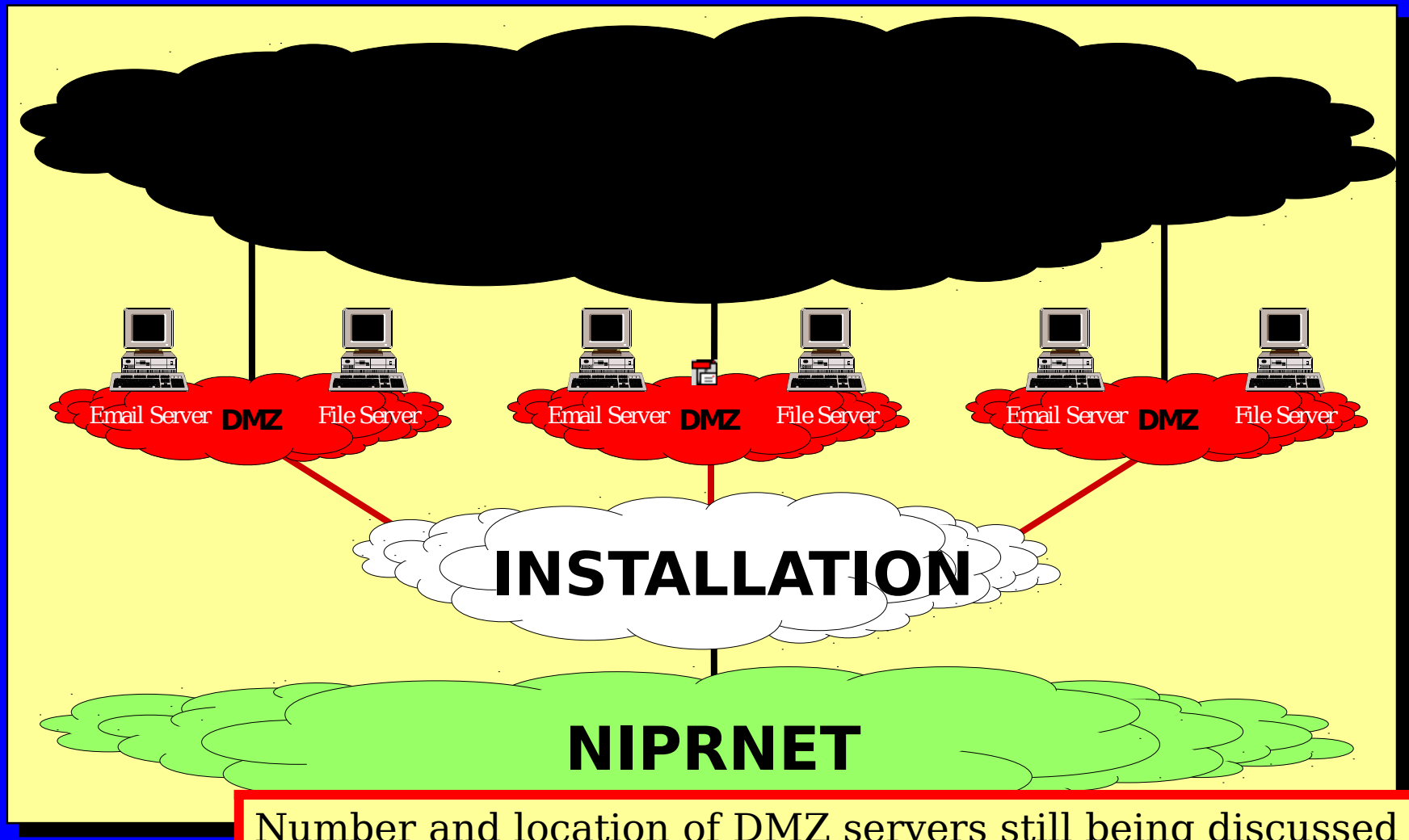
Open NAT Issues

- PKI implementations
  - Certificates for network devices contain the fully qualified domain name of the device
  - Are private devices required to have public certificates?
  - How will this affect user certificates?
- TCP Wrappers
  - Host use TCP Wrappers to secure access to TCP base services
    - Access is defined by IP address or fully qualified domain name
  - Hosts coming from a NAT enclave will have a random IP address and associated fully qualified domain name
    - Static mapping could be used, but would reduce the address space utilization efficiency
  - Investigating the use of Secure Shell or PKI certificates to overcome this issue

Current Recommendations

- Provide additional services in the deployable DMZ/TAPP
  - FTP and SMTP are currently identified as the primary PEO STAMIS data transport protocols
  - Place public service points in the DMZ
    - FTP server, supporting FTP into the enclave
      - Users outside the enclave FTP their files to a designated location on the FTP server
      - Users inside the enclave pull the files off the FTP server
    - Email/SMTP server, supporting receipt and delivery of email
    - Web/HTTP server, potentially
  - Minimizes or eliminates need for static mapping

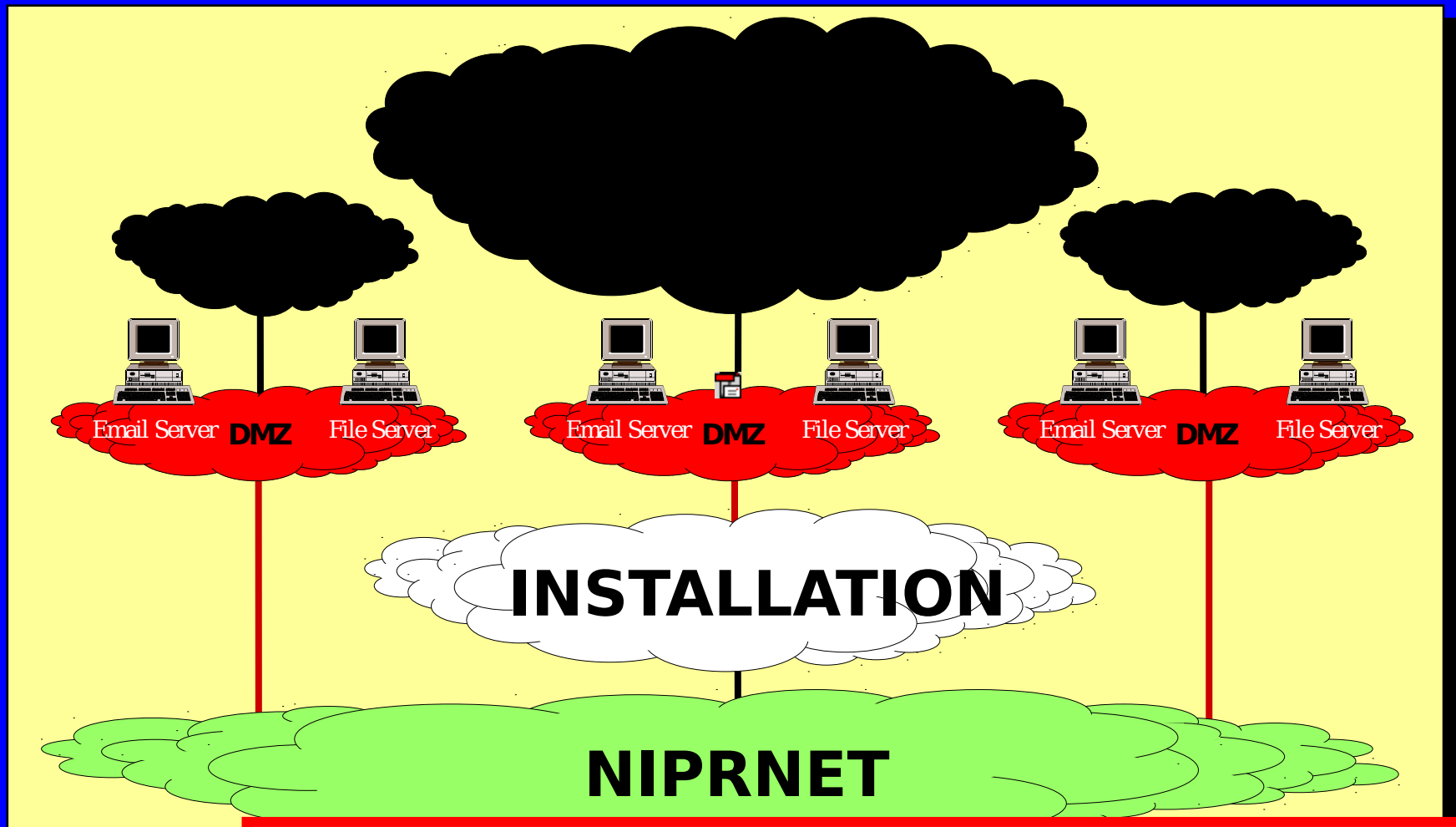
Current Conceptual Enclave - In Garrison



Number and location of DMZ servers still being discussed

MITRE

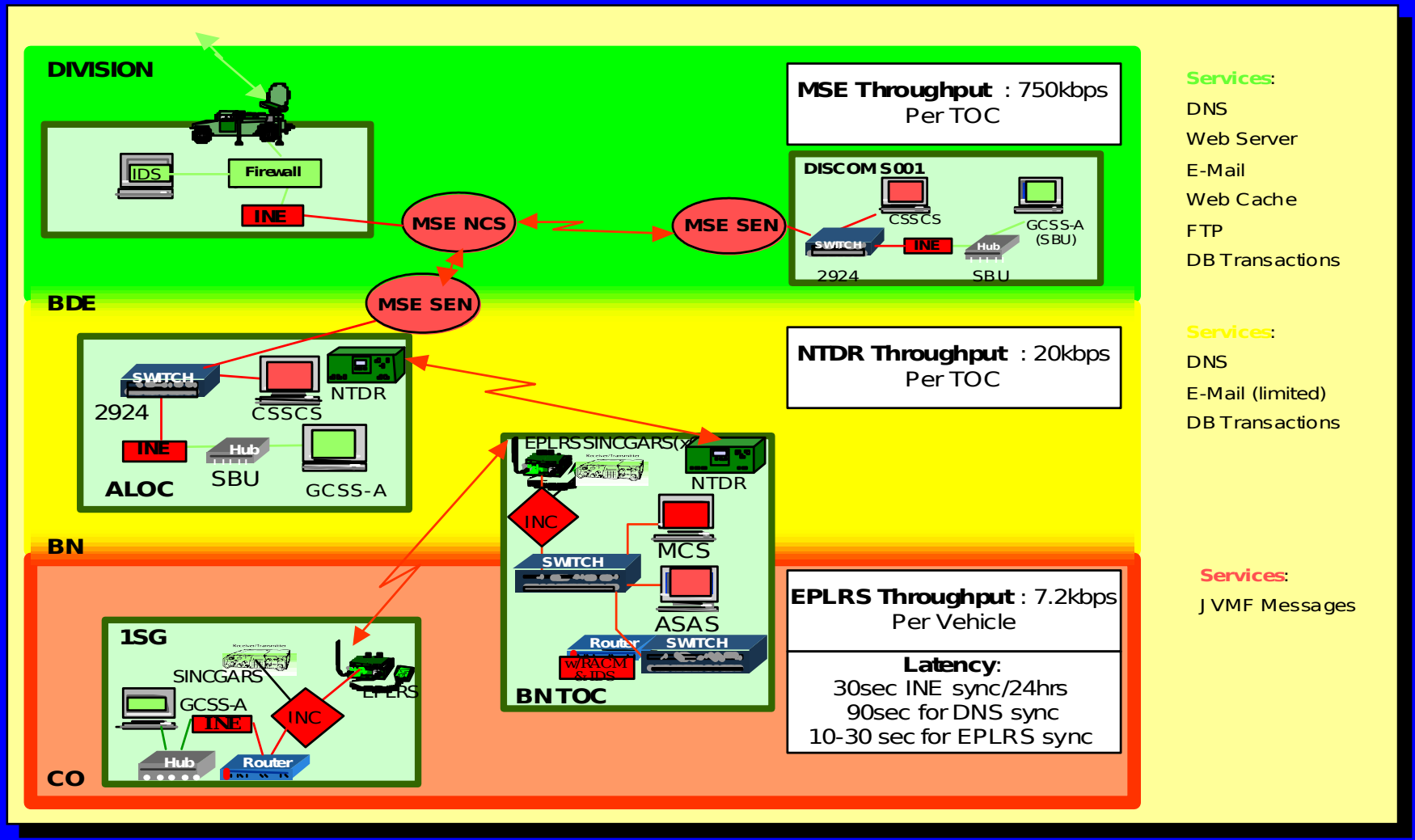
Current Conceptual Enclave - Deployed



Number and location of DMZ servers still being discussed

MITRE

FDD Communications Infrastructure



MITRE

Where are we going

- We will complete our information collection
  - Require the information to ensure we understand the implications of our recommendations
- Complete coordination with other programs
  - PM WIN-T on TAPP
  - PM SET-D
  - PO CAISI
  - PM Directories & Windows 2000 Systems Engineers
  - PEO STAMIS - CIO
- Finalize IPM product recommendations
  - Final IPM test configuration will be a prototype of the recommended IPM configuration
    - Hardware variations may need to be taken into consideration

Questions

MITRE